The background of the slide is a white surface covered with numerous diagonal streaks of various colors, including blue, red, yellow, and purple. These streaks vary in length and thickness, creating a dynamic, abstract pattern.

Esercizio Web Application – preparazione ambiente

Pablo Andres Balbuena
Rios

Esercizio 2

Settimana 3

- ◊ Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Dopo aver Installato in Kali Linux, Bisogna avviare il servizio mysql, nel browser per poterlo attaccare.

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **127.0.0.1**

Operating system: ***nix**

PHP version: **8.2.7**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Enabled**
PHP function allow_url_fopen: **Enabled**
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

Backend database: **MySQL/MariaDB**
Database username: **kali**
Database password: *********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder `/var/www/html/DVWA/hackable/uploads/`: **Yes**
Writable folder `/var/www/html/DVWA/config`: **Yes**


Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

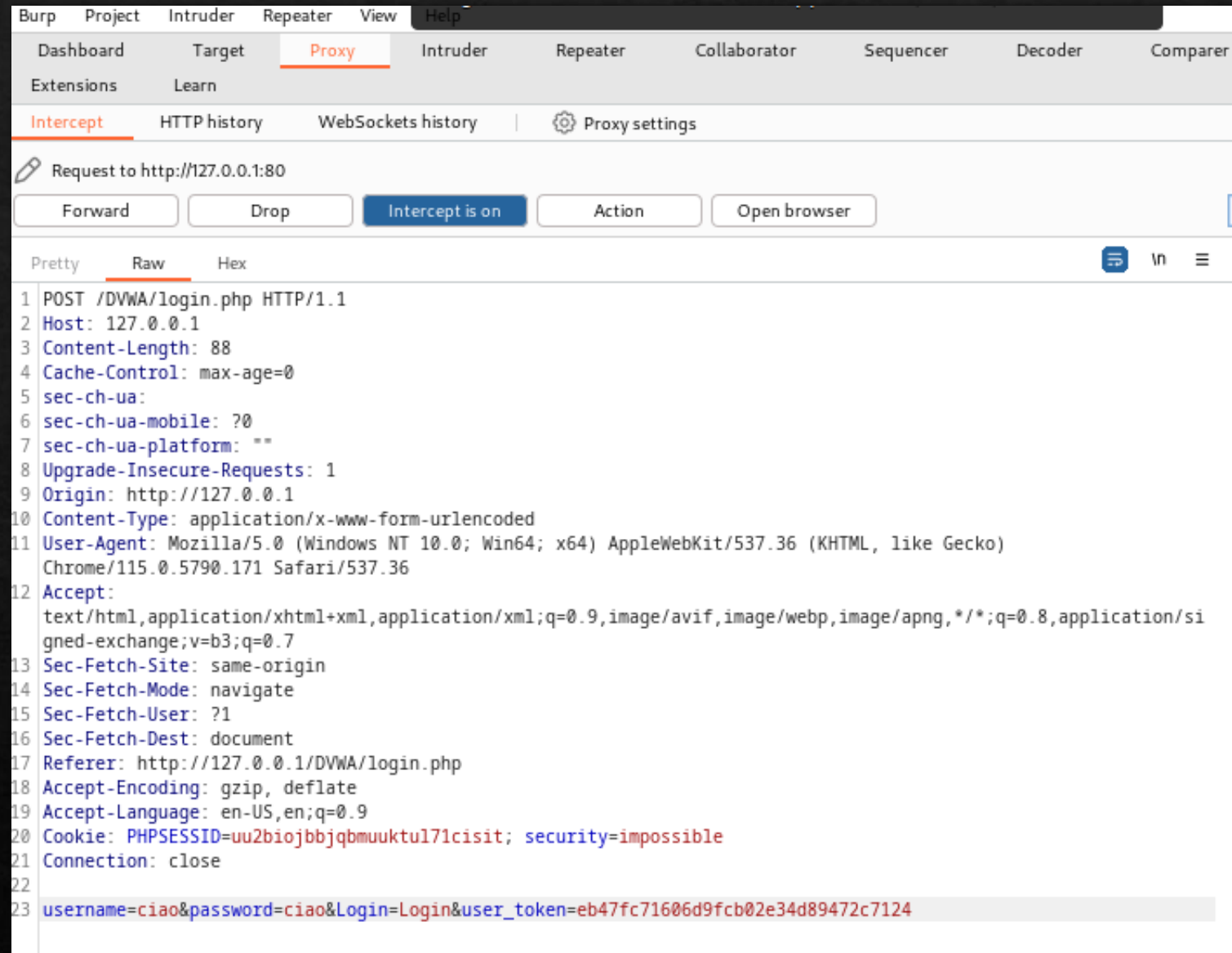
```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

 CTRL (DESTRA)

Bisogna avviare
l'app "Burpsuite",
che
ci permetterà attac
care.



Ho modificato la password e l'username e andato su Repeater per provare a mandare e seguire la direzione

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The main toolbar has buttons for Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, and Comparer. Below the toolbar, there's a section with '1 x' and a '+' button, and a 'Send' button. The main area is split into two panels: 'Request' and 'Response'.

Request

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 83
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: **
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=uu2biojbbjqbmuktul71cisit;
security=impossible
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&user_token=
eb47fc71606d9fcb02e34d89472c7124
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Tue, 12 Dec 2023 16:16:06 GMT
3 Server: Apache/2.4.57 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

Si vede alla fine che il Login
e fallito, attraverso "Login
failed"

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows an HTTP GET request to `/DVWA/login.php` with various headers including `Host: 127.0.0.1`, `Cache-Control: max-age=0`, `sec-ch-ua`, `sec-ch-ua-mobile: ?0`, `sec-ch-ua-platform: ""`, `Upgrade-Insecure-Requests: 1`, `Origin: http://127.0.0.1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`, `Sec-Fetch-Site: same-origin`, `Sec-Fetch-Mode: navigate`, `Sec-Fetch-User: ?1`, `Sec-Fetch-Dest: document`, `Referer: http://127.0.0.1/DVWA/login.php`, `Accept-Encoding: gzip, deflate`, `Accept-Language: en-US,en;q=0.9`, and a `Cookie: PHPSESSID=uu2biojbbjqbmuktu171cisit; security=impossible`. The 'Response' pane on the right shows the HTML output, which includes a `<input type="password">` field, a `<p class="submit">` block with a `<input type="submit" value="Login" name="Login">` button, and a `<div class="message">` block containing the text `Login failed`. The interface also features a top menu bar with options like 'Burp', 'Project', 'Intruder', 'Repeater', 'View', and 'Help', and a bottom search bar.